

NAVAL WAR COLLEGE  
Newport, R.I.

**The United States Homeland Defense Against International Terrorist**

By

A.E. Dochnal

Colonel, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations (JMO).

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Defense.

Signature:\_\_\_\_\_

18 May 2001

Moderators:  
Captain Chester H. Helms  
United States Navy

Professor Donald W. Chisholm

<b>1. Report Security Classification:</b> UNCLASSIFIED			
<b>2. Security Classification Authority:</b>			
<b>3. Declassification/Downgrading Schedule:</b>			
<b>4. Distribution/Availability of Report:</b> DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
<b>5. Name of Performing Organization:</b> JOINT MILITARY OPERATIONS DEPARTMENT			
<b>6. Office Symbol:</b> 1C	<b>7. Address:</b> NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207		
<b>8. Title:</b> UNCLASSIFIED: The United States Homeland Defense Against International Terrorism			
<b>9. Personal Authors:</b> Colonel Alfred E. Dochnal, US Army			
<b>10. Type of Report:</b> FINAL	<b>11. Date of Report:</b> 18 May 2001		
<b>12. Page Count:</b> 24 <b>12A Paper Advisor:</b> None			
<b>13. Supplementary Notation:</b> A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
<b>14. Ten key words that relate to your paper:</b> The United States Homeland defense against international terrorism.			
<b>15. Abstract:</b> <p>The US Unified Commands faces growing potential threats from state actors, their proxies, or independent extremists and terrorists. While various analysts have tended to exaggerate the immediate threat, or the current threat posed by given actors, this does not mean that the threat is not real or that the nation does not need to improve its defense and response capabilities. The US Unified Commands must plan to defend and respond against threats in their respective areas of responsibilities in order to protect American citizens, forces, assets and our allies.</p> <p>The practical problem is to decide how to deal with highly uncertain emerging threats in a world where the US Unified Commands have limited resources, and many other priorities. The US Unified Commands cannot bet the lives and well being of American citizens, forces and allies on today's threats and probabilities. There are many potentially hostile foreign sources of such threats, and some key threats like chemical and biological weapons involve rapidly changing technologies that will pose a steadily growing threat to the US Unified Commands. US Unified Commands involvement in the world and their expansive areas of responsibility make them vulnerable overseas to foreign terrorist attacks. These are dangerous times for the US Unified Commands.</p> <p>Finding the right mix of research and development (new technologies), defense and response is extremely difficult, however, and it is far easier to call for dramatic action than to determine what actions will really succeed and be cost-effective, and executable.</p>			
<b>16. Distribution / Availability of Abstract:</b>	Unclassified <input checked="" type="checkbox"/> X	Same As Rpt	DTIC Users
<b>17. Abstract Security Classification:</b> UNCLASSIFIED			
<b>18. Name of Responsible Individual:</b> CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
<b>19. Telephone:</b> 841-6461	<b>20. Office Symbol:</b> 1C		

Security Classification of This Page Unclassified

## Abstract

# THE UNITED STATES HOMELAND DEFENSE AGAINST INTERNATIONAL TERRORISM: IMPLICATIONS FOR THE JOINT COMMANDER

The United States Unified Commands face growing potential threats from state actors, their proxies and independent extremists and terrorists. While some analysts have exaggerated the immediate threat, or the current threat posted by given actors, this does not mean that the threat is not real or that the nation does not need to improve its defense and response capabilities. The US Unified Commanders must plan to defend and respond against threats in their respective areas of responsibility in order to protect American citizens, forces, assets and our allies.

The practical problem is to decide how to deal with highly uncertain emerging threats in a world where the US Unified Commands have limited resources, and many other priorities. The Joint Force Commanders of these commands cannot bet the lives and well being of American citizens, forces and allies on today's threats and probabilities. There are many potentially hostile foreign sources of such threats, and some key threats like chemical and biological weapons involving rapidly changing technologies that will pose a steadily growing threat. The US Unified Commanders involvement in the world and their expansive areas of responsibility make them vulnerable overseas to foreign terrorist attacks.

The US Unified Commands have the greatest chance of defeating international terrorist by finding the right mix of research and development (new technologies), defense and response that is cost effective and executable.

## **I. Introduction.**

The topic of homeland defense includes a broad array of missions and areas ranging from national missile defense to military assistance to civil authorities. Recently the topic has attracted a great deal of attention due to the public's heightened awareness of the variety and nature of threats addressed in the Hart-Rudman Commission report<sup>1</sup>. This paper will discuss about those areas that address finding the right mix of research and development (new technologies), defense, and approach and response to international terrorism. It is extremely difficult and it is far easier to call for dramatic action than to determine what actions will really succeed and be cost-effective, and executable to combat terrorism.

Defining "Homeland Defense" is the first order of business. There is no definition in JP 1-02 "Department of Defense Dictionary of Military and Associated Terms"<sup>2</sup>. As you can see the US Government needs to develop a comprehensive definition of Homeland defense to provide a uniform basis for coordinating the efforts of all government agencies for deriving mission areas, tasks and responsibilities.

An effective approach to Homeland defense also means that all defenders and responders must understand the range of threats. This will enable the US to deal with more than one attack at a time. Attacks may be coupled to ongoing theater conflicts. Multiple attacks are possible, as are sequential attacks. The Hart-Rudman report highlighted the importance of looking at the link between theater threats and conflicts and attacks on the US, and the threats to our allies and Unified Commands around the world<sup>3</sup>.

The US Unified Commands must also prepare to deal with the first major covert or terrorist attack on the US Unified Commands or its major allies may change the operational

environment fundamentally. The US Unified Commands must begin to both think and act in response to such risks, but a world in which actual attacks occur is one in which the precedent is real and the US Unified Commands defense and response to the first attack will set the precedent to a world in which many similar threats may occur in the future.

The US Unified Commands must broaden the way in which they deal with "Homeland defense" to address all of the tools they have at hand. Approaches to improving Homeland defense arbitrarily exclude US Unified Commands offensive and deterrent capabilities, the ability to defend by identifying and striking at hostile foreign governments and terrorists<sup>4</sup>.

## **II. Chain of Command.**

Each president needs to create the kind of central authority that will ensure the coordination of all federal defense and response activity, develop a common strategy, coordinate program and future year plans and review budget. The precise form this authority takes and whether it should be a cabinet or confirmed position or special assistant to the President is less important than whether it suits the style and needs of a given President. The Department of States Coordinator for Counter Terrorism is Ambassador Michael A. Sheehan and Robert Joseph as the Special Assistant to the President and senior director for Homeland Defense<sup>5</sup>.

At the same time, the US government needs to be less focused on chains of command and be more objective about the need to accept uncertainty and carry out the necessary research, development, and improved planning to reduce that uncertainty. Far too many studies of Homeland defense worry about the issues of "who's in charge" in the federal government, rather than the details of what senior officials should be in charge of. In many

cases, there seems to be an assumption that creating the right organizational chart and set of federal responsibilities can create a mix of authority, capabilities, and liaison efforts with other government agencies and allies.

Finally, putting a new emphasis on Homeland defense is not a reason for creating a new organization or areas of responsibility. The Unified Commands cooperation with our allies and friendly governments is and always will be critical in defending and deterring against terrorists attacks.

### **III. Research and Planning.**

There are many areas where basic research and planning activity is needed to resolve uncertainties, and others where special interest pleading threatens to waste vast amounts of public money on the wrong priorities or measures which may either be ineffective or easy to counter. There have been far more attempts to define broad strategies or issue broad directives than come to grips with the need for detailed planning, adequate programs, and program budgets, and meaningful ways to review and coordinate annual budgets and programs.

There is great deal of planning that needs to be done to thwart major terrorist threats that involve more sophisticated terrorist and extremist groups in the lower-level forms of conventional, chemical, radiological, and biological attacks. These are the "worst case scenarios" today's terrorists seem to pose, and from which form the focus of today's efforts to improve defense and response. Major legal issues concerning international law enforcement compound these problems<sup>6</sup>.

Effective planning and action cannot be based itself on vague calls for improved strategy, exercising and training based on today's threat analyses and techniques, or altering organization charts at the top. In most cases, it is the willingness and ability to address

detailed issues and to make hands on efforts to create and implement a wide range of cost-effective programs that will determine the success of the US Unified Commands efforts in Homeland defense and not the efforts to find a few recommendations. The devil really does lay in the details, and "bumper sticker", or one-issue approaches to policy, are a recommendation for disaster<sup>7</sup>.

#### **IV. Research and Development.**

Effective research and development efforts are needed in virtually every key area of defense and response activity, and indeed to improve the ability to use political, economic, and military actions outside the US Unified Commands to deter and defend against foreign terrorist attacks. At the same time, effective research and development efforts require certain key tools that are sadly lacking in many, if not most, such programs.

There must be a comprehensive and regularly updated net technical assessment of the trends in defensive and offensive technology to establish priorities and the probable cost-effectiveness of given programs. Basic advances are needed in estimating and modeling the chemical and biological threats to determine what research and development (R&D) activities are most needed. Each R&D program requires a clear analysis of how the end result would be deployed and the procurement and life cycle costs of deploying effective national programs. There must be a firm end to using special pleading about the merits of a program against today's threat, and the lack of program by program justification based on analysis of the trends in offense and defense, countermeasures to the proposed or ongoing R&D activity, and the cost to defeat a deployed system<sup>8</sup>. The US Unified Commands must come firmly to grips with the fact it does not exist at the end of history and has not forged a kinder and gentler world.

Unchecked vulnerability is an unacceptable danger for "the world's only superpower." I shudder to think that terrorists should go unchecked. The evolution of more effective Homeland defense is almost certainly essential to deterrence. At the same time, the very term "Homeland defense" can be misleading.

An adequate Homeland defense program must be based on defending and responding to terrorism, extremism, or the kind of limited chemical and biological attacks that now seem most probable. States and more sophisticated non-state groups may attack as well. Advances in biotechnology may give individuals or smaller groups far more lethal weapons in the future.

Counter-terrorism efforts must be closely linked with other government agencies in dealing with these new threats, and it is clear that US Unified Commands must rethink many of their current security concepts. Even the strongest advocates of Homeland defense must recognize that a better offense may often be more effective than improved defense.

Improving the offensive threat of retaliation overseas may often be the best way of defending US interests overseas. A given investment in strengthening our allies may often be a better defense against terrorism than investing in domestic counter-terrorism programs. Hard trade-offs may have to be made between investments in the intelligence needed to intimidate and deter foreign states and terrorist groups, and the international law enforcement cooperation needed to intercept attackers<sup>9</sup>.

The US Unified Commands cannot afford to rely on rethinking the offense as a substitute for improved defense, anymore than it can use defense as a substitute for deterrence, offense, and retaliation. The US Unified Commands can prepare itself for the new threats posed by foreign terrorism using means like chemical, biological, and

information warfare. The world of the 21st Century will not be a repetition of the mutual assured destruction of the Cold War. Radical states, regimes acting under extreme pressure can turn threats like chemical, biological, and nuclear weapons into grim realities in ways the US Unified Commands will never be able to deter<sup>10</sup>.

## **V. Acquisitions.**

The US Unified Commands must take a new approach to research and development and technology to combat international terrorist. There are many areas of new technologies that must be moved off the drawing board, tested, deployed, and modified if the US Unified Commands is to have defensive tools that begin to match its offensive capabilities. At the same time, the US Unified Commands needs careful net assessments of the trends in the threat and how these impact on new approaches to defense and response. Effective planning means that the US Unified Commands cannot afford to mix the myth of technology with the reality. The past track record of US efforts to create and use new technologies in its defense is one of eventual success. At the same time, it is one of almost universal evidence that even the best technologists cannot be trusted to create successful and deployable tools with anything like the promised effectiveness at the promised cost and time.

The development of such a complex approach to threat assessment and program development particularly one that is based on a frank admission of the vast uncertainties involved goes against the basic grain of the American character, and forces far more demanding criteria for program justification than are normally required. The US Unified Commands cannot deal effectively with threats posed by state actors or independent extremists and terrorists unless it adopts such an approach<sup>11</sup>.

Threat analysis needs to be improved by efforts within the joint intelligence research, development, technology and energy (JRDT&E) communities to create annual national threat assessments that evaluate the overall trends in threat technology and methods of attack, and to provide JRDT&E planners with better, and technologically oriented threat forecasts. This should probably take the form of an annual National Intelligence Estimate (NIE) with outside support from a task force composed of cleared JRDT&E experts. It should explicitly consider the risk of a terrorist state, as well as terrorist and extremist attacks, and the linkage between the growing risk of biological attacks, the problems created by changes in the pattern of natural disease, and changes in biotechnology. Two key goals behind such an effort is to educate the intelligence community in the impact of changes in technology, and how to improve warning <sup>12</sup>.

The US Unified Commands must develop and conduct ongoing annual net threat assessments of the foreign and domestic threat of chemical and biological attacks. Threat assessments are not adequate to establish the balance of evolving trends in offensive and defensive technology, and the formulation, prioritization, and execution of successful JRDT&E programs.

Even if the US Unified Commands adopts such an approach, it will still have to concentrate many of its limited resources on making marginal improvements in current capabilities to deal with current threats, while adopting a research and development-driven approach to dealing with more serious and emerging threats. As a result, any US Unified Commands program is likely to have marginal impact, and require constant evolution for at least the next half-decade.

## **VI. Transnational Threats.**

No one can predict that the US Unified Commands are subject to major terrorist attacks using weapons of mass destruction. At the same time, this study has indicated that there is a clear incentive for such attacks and that there are states that could emerge as potential attackers. There is no firm way to assign priorities to the need to fill the gap between "terrorism" and the concern with overt threats like ballistic missiles, but the following factors must be considered:

Low-level terrorist attacks are indeed more probable, and in fact are constantly occurring at the cyber and false alarm level. Seen over a 25-year period and the probability of some sophisticated form of major terrorist attack may be high. This probability not only affects the US Unified Commands, but its allies.

The US Unified Commands faces an enormous challenge in trying to predict and characterize the nature of such threats. There is no "standard distribution curve" or historical precedents of past events that can be used to predict the future<sup>12</sup>.

Crisis or war driven intentions and escalation are extremely difficult to predict. In reacting to the higher levels of threat posed by terrorism, the US Unified Commands must consider the following factors:

- The problems of warning, defense and response differ sharply by level of attack and threat.
- The rules change for all responders as attacks escalate from conventional low-level terrorism ("criminals and crazies") to major levels of damage and casualties:

- A true national emergency involving a nuclear and/or major biological attack will force the Department of Defense into a critical and probably lead role.
- Possible threats can emerge to ruin the basic structure of America's commerce, economic asset abroad.
- Allied targets, US Unified Command forces and businesses overseas, and critical economic facilities can be targeted.
- Health and emergency services at home and abroad are saturated and face potential realities they can only half-anticipate.
- Multiple and sequential attacks become more likely, as are mixes of methods of attack. The possibility of simultaneous attacks on information systems and critical infrastructure will offer terrorist attackers a low cost adjunct to virtually all forms of terrorist and theater warfare.

Within this context, it is important to consider both what terrorist threats and terrorism have in common, and some of the critical differences. The common areas include:

- All threats relate to a wide range of different national security activities as well as a wide range of domestic defense and response efforts.
- All US Unified Commands response risks defending in one area while failing in the others pushes attackers to attack the less defended area.
- Terrorist or terrorist use of weapons of mass destruction create the risk of attacks with effects so costly that response may prove unaffordable, and where it is unclear that technology and systems are available for effective response.

The US Unified Commands should immediately undertake efforts that are not-resource-intensive, such as contingency planning on legal, psychosocial, and even military issues. This

planning should extend to worst case scenarios involving terrorist state attacks, nuclear attacks, and major biological attacks, and involving the use of mixes of agents, multiple attacks, attacks against multiple cities or targets, and sequential and copy-cat attacks<sup>13</sup>.

## **VII. Biological Threats.**

At the same time, there are critical basic differences between the impact of most forms of terrorism. Sophisticated attackers will respond to US Unified Commands defensive measures by shifting their methods of attack to strike at the least defended areas, and developing countermeasures to exploit the weaknesses in any defense. This makes "cost to defeat" and net technical assessment of all defensive programs and options critical.

The situation with biological technology may be radically different. Biological attacks with immune or genetically engineered strains that have unpredictable delays, persistence and symptoms have the ability to defeat treatment and vaccines.

There are many "true believers" who feel that a given threat will or will not materialize in a given form. Given the inherently uncertain nature of predictions as to who is a threat, the means of attack they will use, and the effectiveness of the means of attack they will use, it is almost certain that some of these "true believers" will eventually prove to be right. The problem is that there is no sufficient evidence to say which threats are most important, or to predict the means of attack and level of effectiveness, and that the overwhelming majority of "true believers" will prove to be wrong<sup>14</sup>.

## **VIII Resources.**

There is also an inherent danger in attempting to create a truly coherent program with rigid lines of responsibility, chains of command, and standardized equipment for defense and response. When a truly high degree of uncertainty exists regarding the need for specific

action, enforcing a high degree of coherence from the center may actually interfere with the efficient use of resources. In many cases Unified Commands will achieve a higher capability to deal with uncertainty if they sub-optimize around those marginal steps each can take to improve their existing capabilities to deal with a wide range of threats. This is particularly true in a sharply resource-constrained environment where many potentially desirable actions will remain unfounded until a much clearer pattern of threats emerges.

Resource constraints can be particularly critical when the threats at issue involve a wide spectrum of extremely lethal biological weapons and nuclear weapons. Large amounts of high explosive, chemical weapons, and less lethal biological weapons can produce truly tragic consequences. The level of deterrence, defense, and response pales in terms of cost in comparison with the ability to deter, defend, and respond to the kind of attacks that could involve casualties far in excess of 10,000 Americans and billions of dollars worth of damage<sup>15</sup>.

### **VIII. Intelligence Assessments.**

The US Unified Commands may or may not get warning that the risk of such attacks has increased, and of the form they will take. If it does not, it may benefit from the fact the first such attacks come against its allies or other nations. It is far from clear that the intelligence and analytic tools exist to warn that a possibility is becoming a probability and then a certainty in time to react, and with sufficient clarity to make the joint force commander react. As a result, the US Unified Commands must (a) be prepared to see increasing "possibility" and not just increasing "probability" as strategic warning, and (b) recognize that it needs contingency plans to change its defense and response plans and programs the moment an attack is successful or a pattern of attack becomes probable<sup>16</sup>.

The US Unified Commands cannot afford to focus on dealing with one successful attack or mix of attacks. It must consider the risk of an emerging pattern of terrorist warfare and highly lethal terrorism, and plan for the "morning after." A mentality that treats any catastrophic attack as a strategic defeat, and that does not prepare for immediate action to deal with follow-on attacks, is a recipe for strategic disaster and an incentive for further attack. The US Unified Commands response plans must explicitly recognize these risks and the need to assure the nation, our allies, and our enemies that we will not be paralyzed or panic even if a nuclear or major biological attack succeeds<sup>17</sup>.

New methods of analysis must be developed that examine the present and future balance of offensive, defensive, and response capabilities. They must be supported by adequate net technological assessments, and analysis of countermeasures and costs to defeat all ongoing and proposed federal activities. It is difficult enough to analyze current or near-term risks, but such analysis simply is not adequate. Effective joint programs can take a decade or more to fully implement, and the technology shaping current threats is constantly changing. This is not simply a matter of basic advances like biotechnology, it is a matter of the steadily growing dissemination of the technology equipment needed to produce and deliver large amounts of high explosive, chemical weapons, and biological weapons. Much of the description of potential threats does not explicitly analyze the potential growth or changes in threat technology even when it proposes the adoption of new deterrent, defensive, and response technologies over a period of many years. There's a lack of technological net assessment that is a key not only to identifying and prioritizing effective programs, but to managing them so they don't counter technology growth<sup>18</sup>.

The US Unified Commands must fundamentally reexamine its assessments of the effects of chemical, biological, radiological, and nuclear weapons in the event of various types of terrorist and terrorist attacks. Far too often, the Unified Commands are attempting to address the evolving threat and consequence of each type of chemical and biological attack using dated research and modeling designed for the needs of the Cold War, or which has been developed to deal with selected generic threats rather than conduct a zero-based examination of the current and potential future consequences of chemical and biological attacks.

There is little real analysis of the impact of multiple attacks, sequential attacks, and the longer-term consequences of attacks. The focus is often almost exclusively on deterring, defending, or responding to the first attack. The US Unified Commands focus on terrorism, rather than terrorist warfare has left a major gap in the planning and analysis of Homeland defense between relatively limited terrorist use of chemical and biological weapons and the far more drastic threat from ballistic missile attacks. As a result, most "worst cases" fall fatally short of being real worst cases. There is far too little analysis of the longer-term physical, psychological, economic, political, and strategic impacts of a major successful attack, or of contingencies involving multiple and sequential attacks. Truly new methods of long-term attack like agricultural or ecological attacks receive limited attention<sup>19</sup>.

Unfortunately, the very popularity of the issue of terrorism and weapons of mass destruction also means that there has been a rush to react to potential threats without developing a common definition of the combined threat posed by covert attacks by state actors, terrorist and extremist attacks by foreign groups. There is still insufficient definition of the different kinds of threats those different kinds of weapons of mass destruction pose and how these relate to threats using conventional explosives. In many cases other

government agencies are defining the nature and intensity of the threat to meet their own internal needs and perceptions, or are acting on assumptions that imply a far better ability to predict the future than can possibly exist.

## **IX. Funding.**

These problems are compounded in part by the fact that Office of Budget and Management (OBM) is required to report to the Congress, but there is no central agency charged with creating a plan, program, and budget. The problem is compounded by a host of jurisdictional problems with the Congress, and the lack of a single committee or joint committee structure that could provide a cohesive degree of overview. As a result, there is a large pool of federal reporting on individual problems and issues, but little effort to appraise the overall program<sup>20</sup>.

There are those who would argue that part of the reason for the lack of funding synchronization is security. There are certainly areas like intelligence where detailed program descriptions could compromise security. There are other areas where too detailed a description of US Unified Commands response capabilities could aid an attacker in planning an attack. In broad terms there is little reason to classify most of the information needed to allow outside analysts to fully understand the nature of our efforts.

There's also a tendency to assume short-term solutions can be found to long-term problems, or fund minor palliatives simply for sake of seeming to act. Few, if any, programs provide any picture of what it will cost to fully implement the activities agencies are now beginning. None seem to provide meaningful measures of effectiveness, or any analysis of the current and future costs of "defeating" the capabilities being funded.

To put it bluntly, far too many good ideas seem to have limited substantive value, raise major uncertainties, reflect the reshaping of existing programs to obtain incremental funding, or raise questions about duplication. The funding for counter terrorism has risen from \$6.5 billion in FY1998 to \$8.3 billion in FY2001<sup>21</sup>.

## **X. International Law.**

Foreign movements and governments need to be deterred and the joint force commander must have plans to respond to prevent attacks and limit or respond to follow on attacks. This creates new dilemmas in international law in an era of undeclared wars, as well as highlights the gap in the Unified Commands offensive planning between counter terrorism efforts overseas, conventional warfare, and nuclear retaliation. Creating an effective political, economic, and military capability to respond to an symmetric nuclear or major biological terrorist or foreign terrorist may again do far more to reduce casualties than any practical investment in improved medical care and other physical response capabilities. At the same time, it raises critical issues about attribution, targeting, collateral damage, international law, and international politics that the joint force commanders have only begun to address. It should also be noted in this context that much of the current planning for medical and response treatment focuses on attacks on human beings, and not on attacks on imported livestock, agriculture, or the ecology. This focus probably is valid in reflecting current probabilities, but it ignores critical possible vectors of attack and ones where hostile states or terrorists may develop steadily greater expertise and capability. Attacks on imported agriculture and the ecology offer a subtle form of attack, further compound the problems in attribution and response, and might be conducted as either a long-term form of anonymous attack or quiet revenge long after a crisis seems to be over<sup>23</sup>.

## **XI. Conclusion.**

Technology is unlikely to be a magic bullet for improving intelligence, or operations. Technology can greatly improve joint forces detection, characterization, attribution, and targeting capabilities. However, far more promises are being made than can possibly be kept, and many are repetitions of promises about the same use of new sensors, detection, and characterization equipment during the height of efforts to improve technology. Far too often, promises are made about devices and new analytic techniques like data mining that bare little relation to their real world capability, availability, and cost. In some cases, the technology is being developed as a device or technique without any practical plan to deploy a system to use it or examination of such an effort's cost effectiveness.

This is as true of technology for defense, response, and military operations as for intelligence. Compartmented intelligence, and the need to protect sources and means, often exacerbates these problems. Once again, it must be stressed that improving intelligence is a vital aspect of effective deterrence. Technology offers major potential improvements in Homeland defense, but it must be applied as a system or systems, not a series of uncoordinated increments, and analysis of the cost to deploy technology and means of defeating it needs far more explicit analysis than it currently receives.

Finally, the US Unified Commands needs to close the current gap between counter terrorism and terrorist warfare in ways that go beyond narrowly defined defense and response efforts. Homeland defense should not be defined purely in terms of reactions within the United States. The US Unified Commands must examine ways it can use its offensive capabilities to deter such attacks, and respond to them in ways that will ensure such attacks

are limited in scope or do not occur in the future. Broader solutions and new approaches to theatre strategy can only enhance the US Unified Commands capabilities.

Nunn-Lugar funding needs to be fully extended to biological weapons. Sanctions and arms control and export control regimes like the Biological Weapons Convention, Australia list, Wassener Convention, Chemical Warfare Convention, etc., are vital parts of an effective Homeland defense effort. They all have limits, and these limits generally are far more serious in detecting and preventing the development of small terrorist threats and terrorism than the deployment of large war fighting capabilities. Existing arms control inspection and verification regimes can also act to license the transfer of key nuclear and chemical technologies to suspect countries or countries where terrorists and extremists operate, while they have little impact on the threat of internal terrorism and extremism in a sophisticated military power like the US Unified Commands. Nevertheless, they can be useful tools in creating a more effective approach to Homeland defense.

As has been stressed at the beginning of this paper, and throughout this analysis, the US Unified Commands must both take an all-inclusive approach to Homeland defense against international terrorism and rethink what is sometimes a near isolationist approach. Much of the literature assumes that the US Unified Commands is the primary target of attacks and the only scene of attacks. One classic argument is that the generic nature of the US role as the "world's only super power" makes it the primary target of foreign action. Similarly, there is a tendency to assume that US Unified Commands deterrence, defense, response, and political, economic, and political action can occur as part of a two person, zero sum game.

In actual practice, the US Unified Commands are a target of foreign movements largely as an extension of theater-driven conflicts and tensions where it is often a secondary

target for state and terrorist attacks. This is certainly true today around the world in every US Unified Command. The US Unified Commands are linked to their allies, to coalitions, to regional peace making efforts, or other critical foreign involvements. Even where this is not the case, the US Unified Commands have the greatest chance of defeating international terrorist by finding the right mix of research and development (new technologies), defense and response that's cost effective and executable.

## End Notes

<sup>1</sup> United States Commission on National Security/21<sup>st</sup> Century, National Strategy: A Concert for Preserving Security and Promoting Freedom April 15, 2000, also known as the Hart-Rudman Commission, P.10.

<sup>2</sup> United States Commission on National Security/21<sup>st</sup> Century, National Strategy: A Concert for Preserving Security and Promoting Freedom April 15, 2000; and the Report of the National Commission on Terrorism, Countering the Changing Threat of International Terrorism, The Terrorism Research Center, June 2000. Some critics maintain, however that as dramatic as terrorist attacks are, to call them serious threat to national security is scarcely plausible. John and Karl Muller, “Sanctions of Mass Destruction,” Foreign, Vol. 78, No. 3, May/June 1999, PP.43-53. Patrick Moore, “Is Catastrophic Terrorism Just Strategic Peanuts”, successfully rebuts this view. National Security Law Report, Vol. 22, No. 4, July-August 2000, PP.1, 5-6.

<sup>3</sup> United States Commission on National Security/21<sup>st</sup> Century, National Strategy: A Concert for Preserving Security and Promoting Freedom, Phase III, December 15, 2000; and this report summarizes enough of the commission’s Phase I and Phase II work to establish an intellectual basis for understanding the Phase III report, but does not repeat the text of prior phases in detail. For those who seek fuller background to this report, the Commission’s earlier works should be consulted directly. This is also known as the Hart/Rudman Commission, P.vi.

<sup>4</sup>General Accounting Office, Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations, GAO/TNSIAD-99-135, May 1999, P. 8-10.

<sup>5</sup> Department of State, Office of the Coordinator For Counter Terrorism, Ambassador at Large Michael A. Sheehan, who coordinates all US Government efforts to improve counter terrorism cooperation with foreign governments. He chairs the Interagency Working Group on Counter Terrorism, and the State Department’s task force to coordinate responses to international terrorists incidents. The Coordinator has the primary responsibility for developing, coordinating, and implementing American counter terrorism policy. US Counter Terrorism Policy- First, make no concessions to the terrorists and strike no deals; Second, bring the terrorists to justice for their crimes; Third, isolate and apply pressure on states that sponsor terrorism to force them to change their behavior; and Fourth, bolster the counter terrorism capabilities of those countries that work with the US and require assistance. Washington, DC:

<sup>6</sup> Department of State, Office of the Coordinator For Counter Terrorism, International Terrorism Convention, Terrorism Conventions, Para 11, and Released by the Office of Counter Terrorism, Washington, DC: August 17, 1998.

<sup>7</sup>General Accounting Office, Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations, GAO/TNSIAD-99-135, May 1999, P. 29.

<sup>8</sup>General Accounting Office, Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations, GAO/TNSIAD-99-163, September 1999, P. 8.

<sup>9</sup>General Accounting Office, Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations, GAO/TNSIAD-99-145, April, P. 20.

<sup>10</sup>United States Commission on National Security/21<sup>st</sup> Century, National Strategy: A Concert for Preserving Security and Promoting Freedom, Phase III, December 15, 2000, P.38.

<sup>11</sup>General Accounting Office, Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counter terrorist Programs, GAO/T-NSIAD-00-172, May 4, 2000, P. 6.

<sup>12</sup>General Accounting Office, Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations, GAO/TNSIAD-99-163, September 1999, P. 18-17.

<sup>13</sup> Mark Juergensmeyer, "Understanding The New Terrorism," Current History, (April 2000): PP. 158-163.

<sup>14</sup> See Ken Alibek, Biohazard, New York, Random House, 1999. Russia then had two programs, a long-standing military program and a new program started in the 1970s, which used Russia's biotechnology industry as a front. This was a major effort that included a significant percentage of Russia's life scientist. It was called "Biopreparat", and was extremely secret. Russia developed the capability to produce extremely large amounts of agent and some estimates indicate capacities in the end of the order of hundreds even thousands of tons in a facilities distributed throughout the FSU. Mobilization plans to be able to take all this production from zero to weapons in a relatively short period of time. The current status of this program, and the location of its stockpiles, scientists, equipment and agents are unknown.

General Accounting Office, Biological Weapons: Efforts to Reduce the Former Soviet Union Threat Poses Benefits and Offers New Risks, GAO/NSIAD-00-138, April 2000.

<sup>15</sup> Department of State, Office of the Coordinator For Counter Terrorism, Ambassador at Large Michael A. Sheehan, The Best Homeland Defense is a Good Counter Terrorism Offense, Washington, DC: <http://www.homelanddefense.org>, October 27, 2000,

<sup>16</sup> Department of State, Office of the Coordinator For Counter Terrorism, Patterns of Global Terrorism 2000, Phillip T. Reeker, Acting Spokesman; Edmund J. Hull Acting Coordinator for Counter Terrorism, Washington, DC: April 30, 2001.

<sup>17</sup> General Accounting Office, Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations, GAO/TNSIAD-99-135," May 1999, P. 6,7.

<sup>18</sup> The United States Commission on National Security/21<sup>st</sup> Century, National Strategy: A Concert for Preserving Security and Promoting Freedom, Phase III, December 15, 2000, P.31-38.

<sup>19</sup> John Arquilla, David Ronfeldt, and Michele Zanini, "Terrorism in the Information Age," Current History, (April 2000): PP. 179-187.

<sup>20</sup> Executive Office of the President, Office of Budget and Management, Annual Report to Congress on Combating Terrorism, May 2000.

<sup>21</sup> White House, Office of the Press Secretary, Announcement on Counter terrorism Funding Request, [http://www.state.gov/www/global/terrorism/000517\\_pres\\_funding.html](http://www.state.gov/www/global/terrorism/000517_pres_funding.html), May 17, 2000.

<sup>23</sup> Department of State, Office of the Coordinator For Counter Terrorism, International Terrorism Convention, Terrorism Conventions, Para 11, and Released by the Office of Counter Terrorism, Washington, DC: August 17, 1998

## Bibliography

Alibek, Ken, Biohazard, New York, Random House, 1999.

Anser Services Inc., The Anser Institute For Homeland Security, “Suggested homeland defense readings,” <http://www.homelandsecurity@anser.org>, February 11, 2000,

Arquilla, John, Ronfelst, David and Zanini, Michele, “Terrorism in the Information Age,” Current History, (April 2000).

Department of Defense, Secretary of Defense William S. Cohen, “Annual Report to the President and the Congress,” Washington, DC: 2000.

Department of State, Office of the Coordinator For Counter Terrorism, “Patterns of Global Terrorism 2000,” Phillip T. Reeker, Acting Spokesman; Edmund J. Hull Acting Coordinator for Counter Terrorism, Washington, DC: April 30, 2001.

Department of State, Office of the Coordinator For Counter Terrorism, Ambassador at Large Michael A. Sheehan, “The Best Homeland Defense is a Good Counter Terrorism Offense,” <http://www.homelanddefense.org>, Washington, DC: October 27, 2000.

Department of State, Office of the Coordinator For Counter Terrorism, “International Terrorism Convention,” Terrorism Conventions, Para 11, and Released by the Office of Counter Terrorism, Washington, DC: August 17, 1998.

Executive Office of the President, Office of Budget and Management, “Annual Report to Congress on Combating Terrorism,” Washington, DC: May 2000.

General Accounting Office, “Biological Weapons: Efforts to Reduce the Former Soviet Union Threat Poses Benefits and Offers New Risks,” GAO/NSIAD-00-138, Washington, DC: April 2000.

General Accounting Office, “Statement,” “Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counter terrorist Programs,” GAO/T-NSIAD-00-172, Washington, DC: May 4, 2000.

General Accounting Office, “Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations,” GAO/TNSIAD-99-145, Washington, DC: April 1999.

General Accounting Office, “Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations,” GAO/TNSIAD-99-135, Washington, DC: May 1999.

General Accounting Office, “Combating Terrorism: Issues to Be Resolved to Improve Counter terrorism Operations,” GAO/TNSIAD-99-163, Washington, DC: September 1999.

Juergensmeyer, Mark, "Understanding The New Terrorism," Current History, (April 2000).

Moore, Patrick, "Is Catastrophic Terrorism Just Strategic Peanuts" National Security Law Report, Vol. 22, No. 4, July-August 2000.

Muller, John and Karl, "Sanctions of Mass Destruction," Foreign Affairs Journal, Vol. 78, No. 3, May/June 1999.

U. S. Congress, Report of the National Commission on Terrorism, Countering the Changing Threat of International Terrorism, The Terrorism Research Center, Washington, DC: June 2000.

U. S. Congress, Commission on National Security/21<sup>st</sup> Century, Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom, Washington, DC: April 15, 2000.

U. S. Congress, Commission on National Security/21<sup>st</sup> Century, National Strategy: A Concert for Preserving Security and Promoting Freedom, Phase III, Washington, DC: December 15, 2000.

Vego, Milan N., Operational Warfare, (Newport, R.I.: Naval War College, 2000).

White House, A National Security Strategy for a Global Age (Washington, DC: GPO, 2000).

White House, Office of the Press Secretary, "Statement", "Counter Terrorism Funding Request," [http://www.state.gov/www/global/terrorism/000517\\_pres\\_funding.html](http://www.state.gov/www/global/terrorism/000517_pres_funding.html), Washington, DC: May 17, 2000.

---

